IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

CTD NETWORKS LLC, Plaintiff, **v.** **MICROSOFT CORPORATION**, Defendant.	**No. 6:22-cv-01049-XR**

DEFENDANT MICROSOFT CORPORATION'S RULE 12(b)(6)
MOTION TO DISMISS PLAINTIFF'S COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES AND RULES

INTRODUCTION

CTD Network LLC's ("CTD") complaint lacks any factual basis for accusing Microsoft Corporation ("Microsoft") of infringing the four asserted patents. In scattershot fashion, CTD alleges that Microsoft security software practices certain claims of four patents on distributed security systems, but those allegations are deficient. Despite naming over a dozen separate products, CTD fails to allege that any single product—alone or in combination—practices all of the patents' claims. Moreover, CTD does not plead that Microsoft uses or controls all the necessary components of the claimed security systems. CTD's direct infringement claims fail under established patent law. Accordingly, CTD's complaint should be dismissed under Fed. R. Civ. P. 12(b)(6).

All four asserted patents, U.S. Patent Nos. 8,327,442 (the "'442 patent"), 9,438,614 (the "'614 patent"), 9,503,470 (the "'470 patent"), and 11,171,974 (the "'974 patent"), relate to distributed agent-based models for security monitoring ("SDI-SCAM"). *See* Dkt. 1-1, Exs. A-D. Specifically, the asserted claims cover systems with a network of "agents" that perform specific security functions, including gathering and analyzing information, determining the likelihood of a threat, and generating counteroffensive measures. *Id.*

CTD does not allege that any single Microsoft product meets all limitations of any claim. Instead, CTD resorts to accusing disparate aspects of multiple different and independent security products, but never alleges how (or even whether) they work together to infringe. Moreover, CTD fails to allege the presence of "agents" that each perform all steps required by the asserted claims. *See* Dkt. 1-1, Exs. E-H. CTD further fails to plead factual allegations, other than a boilerplate legal conclusion, showing how Microsoft engages in directly infringing conduct. CTD's failure to identify any infringing products or conduct is cause to dismiss its complaint with prejudice.

STATEMENT OF RELEVANT FACTS

I. CTD Asserts Four Patents on Security Networks

CTD's complaint alleges that Microsoft directly infringes at least one claim of four asserted patents relating to computer security systems: claim 1 of the '442 patent, claim 10 of the '614 patent, claim 1 of the '470 patent, and claim 1 of the '974 patent. *See* Dkt. 1-1, Exs. E-H. Each identified, asserted claim requires a system claim having multiple "agents" on computers that perform various security functions (emphases added):

- *See* Dkt. 1-1, Ex. A ('442 patent), cl. 1: "A distributed security system that protects individual computers in a computer network having a plurality of computers, said system comprising ***individual computers having agents*** associated therewith . . . ."
- *Id.* Ex. B ('614 patent), cl. 10: "A system that detects the state of a computer network having plurality of nodes, said system comprising ***a plurality of distributed agents*** . . . ."
- *Id.* Ex. C ('470 patent), cl. 1: "a system that detects the state of a computer network, comprising "***a plurality of distributed agents*** disposed in said computer network . . . ."
- *Id.* Ex. D ('974 patent), cl. 1: "a system that detects the state of a computer network, comprising "***a plurality of distributed agents*** disposed in said computer network . . . ."

The patents state expressly that having a network of agents is material to the alleged claimed inventions. *See, e.g.*, '442 patent at 2:17-21 ("The basic architectural approach for SDI-SCAM is that each node of a computer network is loaded with an agent capable both of ensuring security at the locality of the machine on which it is installed, and of communicating with other SDI-SCAM agents across the network."); *id.* at 2:59-3:59 (describing in the "Brief Description of Invention" an overview of the SDI-SCAM agents and their security functions).

CTD's complaint does not identify any factual bases for infringement. Dkt. 1 ¶¶ 20, 27, 34, 41. Instead, it attaches claim charts that purport to show its infringement theories. *See* Dkt. 1-1, Exs. E-H.

II. CTD Tries to Accuse Multiple Microsoft Products

CTD's claim charts rely on a hodgepodge of features taken from websites describing several different Microsoft security offerings. The complaint refers generally to "Microsoft's Microsoft Azure and Microsoft Security systems," pointing to a website that lists over 30 Microsoft "security" products. Dkt. 1 ¶ 18 (citing https://www.microsoft.com/en-us/security). The claim charts themselves rely on features cherry-picked from over a dozen different Microsoft security offerings. These include Microsoft Defender for Endpoint, Microsoft Defender for Cloud, Microsoft Defender for Identity, Microsoft Sentinel, and others. *See, e.g.*, Dkt. 1-1, Ex. E.

CTD does not allege that any *single* Microsoft product or service meets all limitations of any asserted claim. Rather, CTD must resort to accusing aspects of a multitude of Microsoft products, arguing that some products meet *certain* limitations of different claims without alleging how they work together to infringe. *See* Dkt. 1-1, Exs. E-H. In so doing, CTD does not allege that one set of "agents" performs all security functions delineated in the claims, despite the claims' requirement that "each said agent" within the network must perform a set of functions. *Compare* Dkt. 1-1, Ex. A cl. 1 ("said system comprising individual computers having agents associated therewith . . . each performing the steps of . . ."), *with* Dkt. 1-1, Ex. E (identifying Microsoft Defender for Endpoint, Microsoft Defender for Cloud, Microsoft Azure, Microsoft Sentinel etc. each performing different, but not all, steps of each claim).

Additionally, CTD does not allege that Microsoft makes, uses, sells, or imports all components of any claimed system and does not provide any factual allegations to support such an allegation. *See* Dkt. 1 ¶¶ 20, 27, 34, 41. Indeed, CTD's allegations concerning Microsoft's purported infringing activity spans only one line in the complaint: "Defendant has, under 35 U.S.C. §271(a), directly infringed, and continues to directly infringe, literally and/or under the doctrine of equivalents, one or more claims, including without limitation at least claim 1 of the '442 Patent,

by making, using, testing, selling, offering for sale and/or importing into the United States Defendant's Accused Products." *Id.* ¶ 20. No further allegations are provided in any of the appended claim charts. Dkt. 1-1, Exs. E-H. For example, CTD does not identify any hardware that Microsoft provides to create the claimed systems, even though hardware is required to meet the system claims. *Id.* Instead, CTD expressly acknowledges that other, unidentified components are required: "Microsoft Azure and Microsoft Security services *together with various equipment, services, components, and/or software* utilized in providing the Microsoft Azure and Microsoft Security services collectively" satisfy the claims. Dkt. 1-1, Ex. E at 4 (emphasis added).[1] Neither the Complaint nor the Claim Charts ever identify the "various equipment, services, components, and/or software" CTD admits is required to satisfy the claims. *Id.*

ARGUMENT

CTD's complaint should be dismissed under Rule 12(b)(6) because it fails to state a plausible claim for direct patent infringement. It cannot identify any products that satisfy all limitations of any patent claim, nor does it allege that Microsoft makes, uses, or sells any infringing system.

I. LEGAL STANDARD

To survive a motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face'." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). Allegations

[1] Counsel for CTD included the same boilerplate allegation against Microsoft in a different case, for a different client and patent, and entirely different accused technology. *See SafeCast Ltd. v. Microsoft Corp.*, No. 6:22-cv-00983-ADA (W.D. Tex. Sept. 19, 2022) (Dkt. 1-1, Ex. B) ("The Microsoft platform together with various equipment, services, components, and/or software utilized in providing the platform collectively include a system as described by the meaning of this claim."). The same boilerplate is also applied in other CTD cases in this court. *E.g.*, *CTD Networks LLC v. Cisco Sys., Inc.*, No. 6:22-cv-01039-XR, ECF No. 1-1 at 70 ("Cisco Cloud Solutions together with various equipment, services, components, and/or software . . . .").

"merely consistent with" liability are insufficient. *See Twombly*, 550 U.S. at 557. To meet the plausibility standard, plaintiff must plead "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged" and its claim must be based on "more than a *sheer possibility*" of liability. *See Iqbal*, 556 U.S. at 678 (emphasis added).

In a patent infringement case, a plaintiff must "explicitly plead facts to plausibly support" its assertions of direct infringement. *See Ruby Sands LLC v. Am. Nat'l Bank of Tex.*, No. 2:15-cv-1955-JRG, 2016 U.S. Dist. LEXIS 83897, at *11-12 (E.D. Tex. June 28, 2016). "There must be some factual allegations that, when taken as true, articulate why it is plausible that the accused product infringes the patent claim." *Bot M8 LLC v. Sony Corp. of Am.*, 4 F.4th 1342, 1352-53 (Fed. Cir. 2021). Failing to show that the accused products plausibly meet all claim limitations renders the allegations insufficient. *See, e.g.*, *De La Vega v. Microsoft Corp.*, No. 19-cv-00612-ADA, 2020 U.S. Dist. LEXIS 116081, at *16 (W.D. Tex. Feb. 7, 2020) ("Because Plaintiff does not include even a short written description of how the accused instrumentalities meet the 'coupling' limitation, his complaint fails to state a claim upon which relief can be granted."). Moreover, a greater level of detail is required for material elements. *See id.* at 1353 (level of detail required depends on "the complexity of the technology, the materiality of any given element to practicing the asserted claim(s), and the nature of the allegedly infringing device"); *see also Vervain, LLC v. Micron Tech., Inc.*, No. 6:21-cv-00487-ADA, 2022 U.S. Dist. LEXIS 54, at *15, 26 (W.D. Tex. Jan. 3, 2022) ("Based on the complexity and materiality of the claims, the Court concludes that pleading infringement . . . will require more than attaching photos of the Accused Products and summarily alleging that each and every limitation is satisfied.").

A plaintiff has the burden of showing that each accused product infringes the asserted claims. *See L&W, Inc. v. Shertech, Inc.*, 471 F.3d 1311, 1318 (Fed. Cir. 2006) ("[Plaintiff] must

make a prima facie showing of infringement as to each accused device . . . ."). For system claims (such as the ones here), direct infringement requires that a single defendant make, use, or sell all portions of the system. *See Centillion Data Sys., LLC v. Qwest Commnc'ns Int'l Inc.*, 631 F.3d 1279, 1288 (Fed. Cir. 2011); *see also Synchronoss Techs. v. Dropbox, Inc.*, 987 F.3d 1358, 1369 (Fed. Cir. 2021) ("Because Drop-box does not provide its customers with any hardware in conjunction with its accused software, Dropbox does not make, sell, or offer for sale the complete invention.").

II. CTD FAILS TO STATE A CLAIM FOR DIRECT INFRINGEMENT

CTD's hodgepodge of allegations fail to put Microsoft on notice of how various different Microsoft security offerings purportedly meet all limitations of the asserted system claims or how Microsoft purportedly engages in directly infringing activity. CTD's allegations are boilerplate, insufficient, and inconsistent, so its complaint should be dismissed.

A. CTD Fails to Identify any Infringing Microsoft Product

CTD's allegations fail to put Microsoft on notice of what products are accused and how they allegedly infringe. As noted above, CTD's claim charts collect various features taken from over a dozen different Microsoft security programs. CTD does little more than embed screenshots of aspects of these different products into a chart with the recitation of claim elements. It neither ties what they do to the claims, nor makes clear how all elements are met by the various products. *See* Dkt. 1-1, Exs. E-H.

This does not suffice when so many different and independent products have been accused of infringement, especially in light of the materiality of the claim elements and the technology at issue. As noted above, the patents state that having a network of "agents" is critical to the inventions. *See, e.g.*, '442 patent at 2:17-21, 2:59-3:59. *Bot M8*, 4 F.4th at 1355 ("While Bot M8 points to different storage components in the allegedly infringing devices, it never says which one

or ones satisfy the mutual authentication limitation."); *see also Vervain, LLC*, 2022 U.S. Dist. LEXIS 54, at *15; *De La Vega v. Microsoft Corp.*, 2020 U.S. Dist. LEXIS 116081, at *16 (dismissing infringement claims as Plaintiff's screenshots failed to explain how defendant practiced "coupling" limitation).

Under governing patent law, a plausible infringement claim requires allegations showing how the accused products meet the claim limitations. *See, e.g.*, *Vervain, LLC*, 2022 U.S. Dist. LEXIS 54, at *9 (granting motion to dismiss where complaint failed to sufficiently plead factual allegations to support a reasonable inference that the accused product practiced the claimed "hot blocks" and "data integrity test" limitations); *De La Vega v. Microsoft Corp.*, No. W-19-CV-00612-ADA, 2020 U.S. Dist. LEXIS 116081, at *15-17 (W.D. Tex. Feb. 7, 2020) (dismissing direct infringement claims for failure to allege "coupling" limitation met by accused products); *Ruby Sands LLC*, 2016 U.S. Dist. LEXIS 83897 at *11-12 (dismissing direct infringement claim "constructed upon a fatally flawed foundation" as no factual allegations "even remotely suggest[ed]" that the defendant sold the product that was alleged to meet the claim limitation). Here, CTD fails these most basic requirements because it does not identify any infringing products.

1. No "Agent" Performs All the Claimed Functions

As explained above, all asserted patents require "agents" on computers that each performs a set of security functions. For example, Claim 1 of the '442 patent requires "a ***system comprising individual computers having agents*** associated therewith that control the associated individual computer, ***each agent performing the steps of*** creating statistical models of usage of the associated individual computer in said computer network" etc. *See* Dkt. 1-1, Ex. A, cl. 1; *see also id.* Ex. B, cl. 10 (requiring a "plurality of *distributed agents . . . said agents* passively collecting, monitoring, aggregating" etc.) (emphasis added); *id.* Ex. C, cl. 1 (requiring a "plurality of *distributed agents . . . each said distributed agent including a microprocessor adapted to . . .*"); *id.* Ex. D, cl. 1 (requiring

"a plurality of distributed agents . . . *each said distributed agent comprising* . . ." (emphases added).

To plead infringement of these claims, CTD bears the burden to allege that the accused products meet these limitations. Infringement causes of action are product-specific. *See L&W, Inc.*, 471 F.3d at 1317-18 (plaintiff not entitled to summary judgment where it merely assumed but did not show that each accused product met the asserted claims). Here, CTD's allegations are fragmented, identifying certain products for some claim elements, and pointing to different products for others, with no allegation those products are sold or used together.

For example, for the '442 patent, CTD acknowledges that claim 1 has at least nine separate elements, which it labels [1a]-[1i]. Dkt. 1-1, Ex. E. But CTD does not allege that any one product meets each of those nine elements. For example, CTD identifies Microsoft Defender for Endpoint ("MDE") for elements [1a], [1c], and [1g], but does not allege, for instance, that MDE practices [1d]-[1f]. *See, e.g.*, Dkt. 1-1, Ex. E.

[1c] gathering and analyzing information relating to current usage of the associated individual computer in said computer network;	Microsoft Defender for Endpoint can collect and process behavioral signals and threat intelligence. Microsoft Azure DDoS Protection can passively monitor traffic patterns. Microsoft Defender for Identity can monitor users, entity behavior, and activities. It can also capture network traffic data. Microsoft Defender for Cloud can passively monitor and collect security data. Microsoft Sentinel can collect and aggregate the data from other Microsoft solutions, including those previously listed.

[1b] creating statistical models of usage of the associated individual computer in said computer network;	Microsoft Defender for Identity can create a behavioral baseline of normal activity for each user and analyze anomalies with its built-in intelligence to create insights. Microsoft Azure DDoS protection can create a model of normal traffic for an application and generate attack analytics and metrics during an attack. Microsoft Sentinel can map network behavior to create a baseline, analyze threats, generate threat intelligence, and look for anomalies in network behavior. Microsoft Defender for Cloud can use machine learning to determine normal activity.

Dkt. 1-1, Ex. E at 5, 7 (identifying MDE, MDC, Microsoft for Identity ("MDI"), and Microsoft Azure DDoS Protection for element [1c], but MDI, Microsoft Azure DDoS Protection, Microsoft Sentinel, and MDC for element [1b]).

Similarly, CTD then points to another product, Microsoft Defender for Cloud ("MDC") for elements [1b]-[1f], but fails to allege that it performs steps identified as [1g]-[1i]:

[1b] creating statistical models of usage of the associated individual computer in said computer network;	Microsoft Defender for Identity can create a behavioral baseline of normal activity for each user and analyze anomalies with its built-in intelligence to create insights. Microsoft Azure DDoS protection can create a model of normal traffic for an application and generate attack analytics and metrics during an attack. Microsoft Sentinel can map network behavior to create a baseline, analyze threats, generate threat intelligence, and look for anomalies in network behavior. Microsoft Defender for Cloud can use machine learning to determine normal activity.

[1g] updating said statistical models of the associated individual computer to reflect the current usage of the associated individual computer in said computer network and the likelihood of intrusion or attack;	Microsoft Defender for Endpoint can collect and process sensor data and then translate them to insights and threat intelligence. Microsoft Azure DDoS Protection can adjust the traffic profile over time with adaptive tuning. Microsoft Sentinel can use machine learning analytics to map network behavior. The following exemplifies this limitation's existence in Accused Systems: Defender for Endpoint uses the following combination of technology built into Windows 10 and Microsoft's robust cloud service:

Id. at 5, 18.

CTD then accuses MDI in '442 patent limitations [1b] and [1c], but *not* for any of limitations [1d] through [1i]:

[1b] creating statistical models of usage of the associated individual computer in said computer network;	Microsoft Defender for Identity can create a behavioral baseline of normal activity for each user and analyze anomalies with its built-in intelligence to create insights. Microsoft Azure DDoS protection can create a model of normal traffic for an application and generate attack analytics and metrics during an attack. Microsoft Sentinel can map network behavior to create a baseline, analyze threats, generate threat intelligence, and look for anomalies in network behavior. Microsoft Defender for Cloud can use machine learning to determine normal activity.

[1d] determining from said information a pattern of usage of the associated individual computer that is consistent with intrusion or attack of the associated individual computer or the computer network;	Microsoft Azure Firewall contains an intrusion detection and prevention system (IDPS) which can look for specific patterns in network traffic. Microsoft Defender for Cloud can analyze data to determine new attack patterns and trends. It also contains fusion analytics which can analyze alerts to determine attack patterns. The following exemplifies this limitation's existence in Accused Systems: Azure Firewall Premium provides advanced capabilities include signature-based IDPS to allow rapid detection of attacks by looking for specific patterns. These patterns can include byte sequences in network traffic, or known malicious instruction sequences used by malware. There are more than 58,000 signatures in over 50 categories which are updated in real time to protect against new and emerging exploits. The exploit categories include malware, phishing, coin mining, and Trojan attacks. **Source:** (https://docs.microsoft.com/en-us/azure/firewall/overview)

Id. at 5-22.

CTD's allegations for the remaining three patents are similarly deficient. Dkt. 1-1, Exs. F-H. Therefore, even assuming for purposes of this motion that CTD's allegations are correct, they do not show that any single product meets all the claim limitations. In short, CTD mixes and matches individual features of products without stating a cohesive infringement theory as to any individual product, and without alleging the products are somehow combined. CTD effectively pleads itself out of court by showing that no Microsoft product infringes.

In a footnote, Plaintiff caveats that "[t]his exemplary claim chart addresses the Accused Products *broadly based on the fact that the Accused Products infringe in the same general way*."

Dkt. 1-1, Ex. E (emphasis added). Not only is this confusing, since CTD accuses entirely different products of infringing, but the footnote also seeks to excuse CTD from the threshold responsibility of providing in its pleadings its understanding of how the products each meet the claim limitations.

Even more troublesome is the fact that CTD's allegations are inconsistent with the claims themselves. CTD does not allege that the agents for each product perform all steps outlined in the claims. *See, e.g.*, Dkt. 1-1, Ex. E at 5-18 (failing to show how the agent for MDE performs each of the steps identified as '442 patent [1b] through 1[g]); *see also id.* at 18-22 (failing to show how the agent for MDC performs steps identified as [1g] through [1i]); Dkt. 1-1, Ex. F at 10-15 (failing to show where MDE agent performs '614 patent [10d]-[10f]); *see also id.* at 3-5 (failing to show that MDC agents are distributed agents designed for adaptive learning and probabilistic analysis disposed in said computer network [10b]); Dkt. 1-1, Ex. G at 10-11 (failing to point to where MDE agent performs '470 patent [1d]); *see also id.* at 11-15 (failing to point to where MDC agent performs [1e]-[1f]); Dkt 1-1, Ex. H at 10-17 (failing to show MDE agent performs '974 patent [1d]-[1g]); *see also id.* at 3-6, 11-12 (failing to show MDC agent meets elements [1b], [1e]). Instead, CTD alleges that different accused "agents" in different products perform the steps outlined in the claims. *See id.* This is contrary to the claim language itself, which explicitly requires the same agents to perform all steps. *See* Dkt. 1-1, Ex. A ('442 patent), cl. 1; Ex. B ('614 patent), cl. 10; Ex. C ('470 patent), cl. 1; Ex. D ('974 patent), cl. 1. As a result, such allegations are insufficient to state a plausible claim. *Bot M8*, 4 F.4th at 1354 ("Where, as here, the factual allegations are actually inconsistent with and contradict infringement, they are likewise insufficient to state a plausible claim.").

These deficiencies extend across all asserted patents and accused products. Such pleadings are unintelligible and inconsistent, and should be dismissed. *Id.* ("[I]t is the *quality* of the

allegations, not the *quantity*, that matters. And unfortunately for [plaintiff], its allegations, which take a 'kitchen sink' approach to pleading, reveal an inconsistency that is fatal to its infringement case . . . .").

2. CTD Fails to Tie Any Accused Products Together

To the extent CTD contends that a combination of products meet the claims' limitations, CTD fails to plead facts sufficient to support that theory. CTD needed to do so, since it failed to plead that any single product practices all the elements of any asserted claim. *See Bot M8*, 4 F.4th at 1353; *TeleSign Corp. v. Twilio*, cv 16-2106-PSG, 2016 U.S. Dist. LEXIS 123516 at *6 (C.D. Cal. Aug. 3, 2016) (finding plaintiff failed to state a claim for infringement when it neither plausibly alleged any one product performed all elements nor that multiple products were used conjunctively to infringe).

CTD fails to allege that various products together meet the limitations. The accused Microsoft products are, according to CTD's own pleadings, different products with varying functions. *See* Dkt. 1-1, Ex. F at 2 (citing https://www.microsoft.com/en-us/security/business/threat-protection) (Microsoft Defender's function is to "[p]revent and detect attacks across identities, endpoints, apps, email, data, and cloud apps," whereas Microsoft Defender for Cloud's function is to "[p]rotect your multi-cloud and hybrid cloud workloads with built-in XDR capabilities. Secure your servers, storage, databases containers, and more."); *see also id.* (citing (https://www.microsoft.com/en-us/security/business/threat-protection?SilentAuth=1). CTD does not allege how these products plausibly work "conjunctively" together to meet the limitations. *See Telesign*, 2016 U.S. Dist. LEXIS 123516, at *8. Plaintiff does not allege that the accused products can even work together, let alone that they are combined and used as the patents require. Thus, CTD's allegations fail to make out a plausible claim for infringement. *See id.*; *Bot M8*, 4 F.4th at 1355 ("Although the FAC alleges that the PS4 contains multiple storage media and multiple

authentication programs, we agree with the district court . . . [that they] do not plausibly allege that gaming information and a mutual authentication program are stored together on the same memory.").

3. CTD Omits Limitations Specific to the '442 and '470 Patents

In addition to the deficiencies above, CTD fails to allege that *any* products meet certain claim limitations of the '442 and '470 patents. The '442 patent requires "potential countermeasures" distributed to agents, under limitation "[1f]." *See* Dkt. 1-1, Ex. E at 16-17. However, CTD does not identify any such countermeasures in its claim chart, giving Microsoft no notice about what it accuses.

Additionally, the '470 patent requires a "server" that purportedly provides a "security and validity score," and the "reputation of a programmer" that is purportedly a component of this "security and validity score" (limitations [1g] and [1j]). *See* Dkt. 1-1, Ex. G. CTD does not identify anything that corresponds to those components. *Id.* These limitations present independent reasons why the pleadings for the '442 and '470 patents are deficient.

Courts routinely grant motions to dismiss for failure to state a claim in such circumstances where the plaintiff simply omits claim limitations. *See, e.g.*, *Vervain, LLC*, 2022 U.S. Dist. LEXIS 54, at *9 (granting motion to dismiss where complaint failed to sufficiently plead factual allegations to support a reasonable inference that the accused product practiced the claimed "hot blocks" and "data integrity test" limitations); *De La Vega v. Microsoft Corp.*, No. W-19-CV-00612-ADA, 2020 U.S. Dist. LEXIS 116081, at *15-17 (W.D. Tex. Feb. 7, 2020) (dismissing direct infringement claims for failure to allege "coupling" limitation met by accused products); *Ruby Sands LLC*, 2016 U.S. Dist. LEXIS 83897 at *11-12 (dismissing direct infringement claim "constructed upon a fatally flawed foundation" as no factual allegations "even remotely

suggest[ed]" that the defendant sold the product that was alleged to meet the claim limitation). These omissions further show that CTD's allegations are fatally incomplete.

B. Microsoft Does not Infringe any Asserted Patent

In addition to its failure to identify any product that satisfies the claims, CTD fails to allege that Microsoft performs any infringing conduct. For each patent, CTD pleads that Microsoft alone directly infringes by "making, using, testing, selling, offering for sale, and/or importing into the United States Defendant's Accused Products." Dkt. 1 ¶¶ 20, 27, 34, 41. Those assertions are devoid of any supporting factual allegations. For this reason alone, CTD's claims fail. *See Iqbal,* 556 U.S. at 678 ("Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice."); *see also Vervain, LLC*, 2022 U.S. Dist. LEXIS 54, at *5 ("Under any standard . . . the complaint must support its entitlement to relief with 'factual content,' not just conclusory allegations that the accused product(s) meet every claim limitation.").

Regardless, CTD's allegation is also implausible as a matter of law. Even if the claimed security systems exist, Microsoft does not perform acts that constitute infringement. Under U.S. patent law, "whoever without authority makes, uses, offers to sell, or sells any patented invention, within the United States or imports into the United States any patented invention during the term of the patent therefor, infringes the patent." 35 U.S.C. § 271(a). CTD cannot plausibly allege that Microsoft conducts any of these activities.

1. CTD Fails to Allege Making

As a matter of law, in order to "make" a system under § 271(a), Microsoft "would need to combine all of the claim elements." *Centillion*, 631 F.3d at 1288; *see also Personal Audio, LLC v. Google LLC*, No. 1:17-cv-01751 (D. Del. Jan. 7, 2022) (Dkt. 506) at 14 ("Generally, to 'make' a patented device under § 271(a), a single entity must 'combine all of the claim elements'.") (collecting cases) (report and recommendation, adopted by the Court, Dkt. 714). For system

claims that include both hardware and software components, the software producer does not "make" the system. *See Acceleration Bay LLC v. 2k Sports, Inc.*, 15 F.4th 1069, 1078 (Fed. Cir. 2021) ("Acceleration Bay proffers a novel theory . . . that the defendants are liable for 'making' the claimed hardware components even though they are in fact made by third parties, because their accused software runs on them. . . . We disagree."); *Centillion*, 631 F.3d at 1288 (defendant did not combine all claim elements when "customer, not [defendant], completes the system by providing the 'personal computer data processing means' and installing client software."); *Personal Audio*, No. 1:17-cv-01751 (Dkt. 506) at 17 (defendant cannot be liable where "the undisputed evidence demonstrates that it is the *end users* of the accused third-party products who choose whether to receive all updates and/or particular updates pushed by Google.") (emphasis in original).

Here, Microsoft does not make or combine all the elements of the claimed systems. At minimum, Microsoft does not provide hardware components required by the claims. *See* Ex. A at cl. 1 ("system comprising *individual computers* having agents associated therewith"); Ex. B at cl. 10 ("system comprising a plurality of distributed agents . . . said agents . . . alerting other agents, *a central server"*); Ex. C at cl. 1 ("a system . . . comprising: a plurality of distributed agents, each said distributed agent including a *microprocessor* . . . and *means for communicating* at least the aggregated data to other distributed agents"); Ex. D at cl. 1 ("[a] system . . . comprising . . . a plurality of distributed agents disposed in said *computer network*.") (emphases added). Indeed, CTD admits that additional pieces are needed: "Microsoft Azure and Microsoft Security services *together with various equipment, services, components, and/or software utilized* in providing the Microsoft Azure and Microsoft Security services *collectively include a system and method* for a

distributed application and network security system (SDI-SCAM) as described by the meaning of this claim." Dkt. 1-1, Ex. E at 4 (emphasis added).

For example, in the context of both Microsoft Defender for Endpoint and Microsoft Defender for Cloud, customers control the network and the endpoints (individual computers) where the software operates. The customer controls where and how the software is deployed. *See* Ex. E at 3, 7, 18, 19, 20, 21, 22; Ex. F at 3, 5, 7; Ex. G at 3, 5, 7, 15, 16, 19; Ex. H at 3, 5, 7, 20 (citing https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide) ("MDE Documentation," Smith Decl. Ex. 1); MDE Documentation at 3 ("To further reinforce the security perimeter of *your* network"); *id.* at 5 ("[Y]ou can understand Defender for Endpoint and how it can help prevent, detect, investigate, and respond to threat across *your organization's endpoints – your devices and systems"*); *id.* at 1 ("send this sensor data to *your private*, isolated, cloud instance of Microsoft Defender for Endpoint") (emphases added). In using Microsoft Defender for Cloud, customers choose to deploy the software in their privately-controlled cloud resources. *See* Ex. E at 8; Ex. F at 2, 8; Ex. G at 2, 8; Ex. H at 2, 8 (citing https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction) ("MDC Documentation," Smith Decl. Ex. 2); MDC Documentation at 1 ("Microsoft Defender for Cloud is a Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) for all your Azure, on-premises and multicloud (Amazon AWS and Google GCP) resources."). Of course, Microsoft does not control how a customer configures agents within systems on its own premises or in other cloud providers. And even in Azure, the customer still controls the configuration of agents. *See* MDC Documentation at 10 ("Use the advanced protection tiles in the workload protections dashboard to monitor and configure each of these protections."). In both cases, while a customer may be using Microsoft

software, the customer dictates how the software is run in its chosen hardware environment and, therefore, Microsoft cannot be held liable for "making" a system that includes both the accused software and hardware. *Acceleration Bay*, 15 F.4th at 1078.

2. CTD Fails to Allege Use

As a matter of law, CTD's allegations regarding Microsoft's "use" of an infringing system are also flawed.[2] CTD contends that the "Microsoft Azure and Microsoft Security services are made available by a system owned and/or operated by Microsoft," and that "'infringement is not dependent on ownership of all limitations of a claim." Dkt. 1-1 at 4. However, these statements are legally incorrect. As the Federal Circuit has explained, "use" of a system requires more: "We hold that to 'use' a system for purposes of infringement, a party must put the invention into service, *i.e.*, control the system as a whole and obtain benefit from it." *Centillion*, 631 F.3d at 1285. Under very similar facts, *Centillion* held that providing software for a computer system is not "use," as only customers "use" the system. *Id.* at 1286 ("Supplying the software for the customer to use is not the same as using the system."). "While Qwest may make the backend processing elements, it never 'uses' the entire claimed system because it never puts into service the personal computer data processing means. Supplying the software for the customer to use is not the same as using the system." *Id.*

Here, Microsoft does not put the system "into service." It does not deploy or control the recited "agents" that are associated with the protected network or network devices. *See* Ex. A at cl.1 ("system comprising *individual computers having agents associated therewith*"); Ex. B at cl. 10 ("system that detects the state of a computer network having a plurality of nodes, said system

[2] To the extent CTD contends that Microsoft's alleged "testing" constitutes "use," then its allegation regarding testing is entirely redundant of its allegation of use, and is addressed by Microsoft's arguments concerning use. CTD also identifies no actual instance of testing.

comprising a *plurality of distributed agents*"); Ex. C at cl. 1 ("a system . . . comprising: *a plurality of distributed agents*, each said distributed agent including a microprocessor"); Ex. D at cl. 1 ("[a] system . . . comprising . . . *a plurality of distributed agents* disposed in said computer network . . . and means for communicating at least the aggregated data to other distributed agents.") (emphases added). As explained above, the complaint does not allege that Microsoft supplies individual computers or agents, which the patents require.

For example, with respect to the accused Microsoft Defender for Endpoint, *customers* control the deployment. *See* Ex. E at 3, 7, 18, 19, 20, 21, and 22; Ex. F at 3, 5, 7; Ex. G at 3, 5, 7, 15, 16, and 19; Ex. H at 3, 5, 7, and 20 (citing MDE Documentation); *see also* MDE Documentation at 3 ("To further reinforce the security perimeter of *your* network."); *id.* at 5 ("[Y]ou can understand Defender for Endpoint and how it can help prevent, detect, investigate, and respond to threat across *your organization's endpoints – your devices and systems*"); *id.* at 1 ("send this sensor data to *your private*, isolated, cloud instance of Microsoft Defender for Endpoint") (emphases added). Put simply, Microsoft cannot control whether or how customers use Microsoft Defender for Endpoint software in their devices or networks—or even whether customers turn on their computers. Thus, it cannot infringe by putting the system "into service."

Similarly, with respect to Microsoft Defender for Cloud, the customer controls the cloud resources where the alleged "agents" are deployed. *See* Ex. E at 8; Ex. F at 2, 8; Ex. G at 2, 8; Ex. H at 2, 8 (citing MDC Documentation at 1 ("Microsoft Defender for Cloud is a Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) for all your Azure, on-premises and multicloud (Amazon AWS and Google GCP) resources."). Microsoft does not control how the customer deploys or uses the Microsoft Defender for Cloud software on the customer's premises or in their own chosen cloud environment. Thus, as with the Microsoft

Defender for Endpoint products, Microsoft does not control a portion of the recited systems and, therefore, cannot directly infringe by putting the system into service.

3. CTD Fails to Allege Sale or Importation

To infringe through the sale of an accused system, "all of the elements of the claim [must be] present in the accused system[s] allegedly sold." *See Omega Patents, LLC v. CalAmp Corp.*, 920 F.3d 1337, 1344 (Fed. Cir. 2019); *ESW Holdings, Inc. v. Roku, Inc.*, No. 6-19-CV-00044-ADA, 2021 U.S. Dist. LEXIS 51731, at *14-15 (W.D. Tex. Mar. 18, 2021) (granting summary judgment for no infringement where "Roku does not make, sell, or offer to sell the entire system recited in [the asserted] claim . . . it only makes, sells, or offers to sell a part of the system"). CTD's allegations fail to state a plausible claim for infringement for several reasons.

First, CTD fails to allege that certain accused services are actually sold. *See e.g.*, Ex. E at 7, Ex. F at 7, Ex. G at 7, Ex. H at 7 (discussing "Cloud security analytics"). An offer of services to the benefit of the customer does not constitute a sale or offer for sale. *See NTP, Inc. v. Research In Motion, Ltd.*, 418 F.3d 1282, 1321 (Fed. Cir. 2005) (stating performance of claim steps as a service for its customers cannot be considered a sale or an offer to sell an invention); *see id.* at 1319 ("[T]he ordinary meaning of a sale includes the concept of a transfer of title or property. The definition also requires as the third element 'a thing capable of being transferred.'").

Second, Microsoft does not sell the necessary hardware components. Ex. A at cl. 1 ("system comprising *individual computers* having agents associated therewith"); Ex. B at cl. 10 ("system comprising a plurality of distributed agents . . . said agents . . . alerting . . . a *central server*"); Ex. C at cl. 1 ("a system . . . comprising: a plurality of distributed agents, each said distributed agent including a *microprocessor* . . . and means for communicating at least the aggregated data to other distributed agents"); Ex. D at cl. 1 ("[a] system . . . comprising . . . a

plurality of distributed agents disposed in said *computer network*.") (emphases added). For example, the claimed computer, the central server, the claimed microprocessor, the claimed means for communicating, and the claimed computer network belong to the user. Microsoft offers software, which the customer deploys on its customer-controlled hardware when using Microsoft Defender for Endpoint, and on its privately controlled cloud platform (whether it be customer-owned, third-party owned, or Microsoft-owned) when using Microsoft Defender for Cloud. Microsoft never transfers title or control of any hardware to the customer. Thus, Microsoft cannot sell the claimed system when providing its software products and services.

Lastly, the complaint fails to state any claim that Microsoft directly infringes by "importing" the accused products. For the same reasons that Microsoft does not sell any patented systems, Microsoft does not import "a distributed security system . . . in a computer network." Dkt. 1-1, Exs. A-D. Nor is it clear how Microsoft would import certain components such as "agents" or "distributed adaptive machine learning model[s]. *See, e.g.*, Dkt. 1-1, Ex. D ('974 patent) at cl. 1 ("each said distributed agent comprising . . . a distributed adaptive machine learning model that analyzes the aggregated data . . ."); Dkt. 1-1, Ex. C ('470 patent) at cl. 1 ("a server that provides a security and validity score . . ."). As there is no reasonable suggestion that Microsoft can import the components claimed, the Court is entitled to draw on its "judicial experience and common sense" and dismiss the claim. *See Juniper Networks, Inc. v. Shipley*, 643 F.3d 1346, 1352 (Fed. Cir. 2011) (affirming Rule 12(b)(6) dismissal).

III. DISMISSAL WITH PREJUDICE IS WARRANTED AS ANY AMENDMENT WOULD BE FUTILE

CTD's own omissions and allegations reflect its recognition that Microsoft's products do not satisfy all limitations of the asserted claims, and that Microsoft does not "control" the allegedly claimed system. Based on the variety of allegations in CTD's complaint, CTD has had ample time

to scour publicly available information about Microsoft's various security offerings and was still unable to identify any Microsoft product that satisfies each element of any asserted claim. Thus, CTD cannot correct its flawed allegations. Any amendment would be futile, and the complaint should be dismissed with prejudice. *See Burke v. Ocwen Loan Servicing*, 855 F. App'x 180, 187 (5th Cir. 2021); *Valdez v. Victory Med. Ctr. Southcross*, No. SA-16-CA-1016-FB, 2016 U.S. Dist. LEXIS 202250, at *13 (W.D. Tex. Dec. 12, 2016).

CONCLUSION

For these reasons, Microsoft respectfully requests dismissal of CTD's complaint in its entirety with prejudice.

Dated: December 30, 2022

Respectfully submitted,

/s/ Melissa R. Smith

Melissa R. Smith
State Bar No. 24001351
GILLAM & SMITH, LLP
303 South Washington Avenue
Marshall, Texas 75670
Tel: (903) 934-8450
Fax: (903) 934-9257
melissa@gillamsmithlaw.com

Jonathan J. Lamberson (*pro hac vice pending*)
Henry Huang (*pro hac vice pending*)
WHITE & CASE LLP
3000 El Camino Real
2 Palo Alto Square, Suite 900
Palo Alto, CA 94306
Tel: (650) 213-0300
lamberson@whitecase.com
henry.huang@whitecase.com

Lauren Kuehn Pelletier *(pro hac vice pending)*
WHITE & CASE LLP
1221 Avenue of the Americas
New York, New York 10020
Tel: (212) 819-8200
lauren.kuehn@whitecase.com

Attorneys for Defendant Microsoft Corporation

CERTIFICATE OF SERVICE

The undersigned certifies that on December 30, 2022, I electronically filed this document with the Clerk of Court via the Court's CM/ECF system which will send notification of such filing to all counsel of record, all of whom have consented to electronic service in this action.

/s/ Melissa R. Smith
Melissa R. Smith